

7. How can you configure scan policies and templates in Nessus?

Configuring Scan Policies and Templates in Nessus

In **Nessus**, **Scan Policies and Templates** allow you to customize how scans are performed, ensuring you get accurate and relevant security insights. Proper configuration enhances scan performance and helps avoid unnecessary noise in results. 🚀

1. Understanding Scan Policies & Templates

- **Scan Template:** A predefined scanning configuration for common security needs.
- **Scan Policy:** A **customized scan configuration** that allows full control over scanning behavior.

2. Configuring Scan Policies in Nessus

A **Scan Policy** lets you **customize** settings like **targets, ports, performance, and security checks**.

Steps to Create a Custom Scan Policy

- 1 **Log in to Nessus** (`https://localhost:8834`)
- 2 Click on **"Policies"** in the left menu
- 3 Click **"New Policy"**
- 4 Choose a **Scan Type** (Basic Network, Advanced, Web App, etc.)
- 5 Configure policy settings (**see breakdown below**)
- 6 Click **"Save"**

✅ **Pro Tip:** Use **Advanced Scan** for full control over **scan depth, credentials, and safe checks**.

3. Key Scan Policy Settings

When creating a policy, you can configure the following:

A. General Settings

Setting	Description
Name	Policy name (e.g., "Internal Network Scan")
Description	Short details of what the scan does
Folder	Organize policies into different categories

Setting	Description
Visibility	Choose Private (only you) or Shared (team access)

B. Targets & Discovery

Setting	Description
Scan Targets	Specify IP addresses, ranges, or domain names
Host Discovery	Finds live systems before scanning
Port Scanning	Choose SYN scan, TCP scan, or Ping sweep

✔ **Best Practice:** Use **Host Discovery** to **reduce scan time** by avoiding inactive hosts.

C. Vulnerability Assessment

Setting	Description
Vulnerability Checks	Choose between Safe Mode (low risk) or Aggressive Mode (deeper scanning, may crash systems)
Authentication (Credentialed Scans)	Uses SSH, RDP, or SMB credentials for deeper scanning
Malware Detection	Scans for backdoors, botnets, and rootkits
Web Application Scanning	Detects SQL Injection, XSS, LFI/RFI, and OWASP Top 10

✔ **Best Practice:** Use **Credentialed Scanning** for deeper insights into **system vulnerabilities**.

D. Performance & Optimization

Setting	Description
Scan Speed	Choose Low (Safe), Normal, or Aggressive (Faster but riskier)
Parallel Hosts	Defines how many hosts Nessus scans at once
Max Checks per Host	Limits the number of checks per host
Network Timeout	Adjust timeout settings for slow networks

✔ **Best Practice:** Use **"Normal" scan speed** for **accurate and efficient** scanning.






◆ 4. Configuring Scan Templates

Nessus provides **prebuilt scan templates** for different scanning needs.

How to Select & Customize a Scan Template

1 Click **"Scans" > "New Scan"**

2 Choose a **Scan Template**:

-  **Basic Network Scan** → General vulnerability scanning
-  **Advanced Scan** → Full control over scanning settings
-  **Web App Scan** → Identifies web security flaws
-  **Credentialed Patch Audit** → Finds outdated software
-  **Host Discovery Scan** → Finds active hosts on a network

3 Click **"Save"** or **"Launch"**

✓ **Best Practice:** Use **"Basic Network Scan"** for quick checks & **"Advanced Scan"** for deep analysis.

◆ **5. Managing & Applying Policies**

Once you've created a **Scan Policy**, you can use it in your scans.

How to Apply a Custom Scan Policy

1 Go to **"Scans" > "New Scan"**

2 Click **"My Scan Policies"** (instead of templates)

3 Select your **Custom Policy**

4 Enter **Target IPs** & adjust settings

5 Click **"Save"** or **"Launch"**

✓ **Pro Tip:** Apply custom policies **only to specific systems** to avoid unnecessary scanning.

Final Tips for Nessus Policy Optimization

- ✓ **Use Host Discovery** to reduce scan time
- ✓ **Enable Credentialed Scans** for deeper results
- ✓ **Set Safe Mode** on **production environments** to avoid crashes
- ✓ **Limit Network Traffic** for high-performance scans
- ✓ **Use Scheduled Scans** to automate scanning